



Homeland
Security

Daily Open Source Infrastructure Report

13 April 2015

Top Stories

- A \$1.6 billion penalty was issued to Pacific Gas & Electric Company April 9 for a 2010 fatal gas-pipeline explosion in California that killed 8 people and destroyed a neighborhood. – *San Jose Mercury News* (See item [1](#))
- The former controller of Illinois-based Molex Japan Co. Ltd., was charged April 9 after he allegedly caused the company \$201.9 million in net losses through unauthorized equity trading. – *U.S. Securities and Exchange Commission* (See item [5](#))
- Law enforcement organizations and private security companies worked to disrupt the Changeup worm botnet and sinkhole its command-and-control (C&C) servers after the worm leveraged a LNK vulnerability in Windows, infecting 30,000 systems in early 2015. – *Softpedia* (See item [25](#))
- Severe storms April 8-9 damaged about 15 buildings in the St. Louis area, and caused damage to about 50 structures in Fairdale, Illinois. – *St. Louis Post-Dispatch* (See item [30](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *April 10, San Jose Mercury News* – (California) **PG&E slapped with record \$1.6 billion penalty for fatal San Bruno explosion.** The California Public Utilities Commission announced April 9 that it issued a \$1.6 billion penalty to Pacific Gas & Electric Company for a 2010 fatal gas-pipeline explosion in San Bruno that killed 8 people and destroyed a neighborhood.
Source: http://www.mercurynews.com/business/ci_27880159/san-bruno-pg-e-faces-record-penalty-punishment
2. *April 9, Forum of Fargo-Moorhead* – (North Dakota) **Equipment malfunction caused Killdeer explosion, investigation finds.** Marathon Oil announced April 9 that the cause of a March 7 oil tank explosion near Killdeer that spilled 244 barrels of oil and 45 barrels of saltwater was caused by an equipment malfunction when an in-line flame arrestor failed and allowed the flare flame to get into the tanks. The company stated that it will thoroughly check the arrestors during future inspections.
Source: <http://www.inforum.com/news/3718917-equipment-malfunction-caused-killdeer-explosion-investigation-finds>

For another story, see item [30](#)

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

3. *April 8, KARK 4 Little Rock* – (Arkansas) **Radioactive gauge stolen from Pulaski Co. construction site found.** The Arkansas Department of Health reported April 8 that a radioactive gauge containing small amounts of radioactive material that was stolen March 30 from a Pulaski County construction site was found undamaged near the Marche community, and was transported to a permanent storage location.
Source: <http://www.arkansasmatters.com/story/d/story/update-radioactive-gauge-stolen-from-pulaski-co-co/20797/XxtVK6NaLk6HJQq3BVzBQg>

[\[Return to top\]](#)

Critical Manufacturing Sector

4. *April 10, Detroit News* – (National) **Nissan, BMW recall 94,000 '14 vehicles for fuel pump.** Nissan Motor Co., and BMW AG issued a recall April 10 for 76,242 model year 2014 Nissan Rogue SUVs and 18,054 model year 2014 BMW cars of various models, due to improper nickel plating of components within the fuel pump that could cause

Nissan vehicles to fail to start and launched an investigation into the issue by BMW's fuel pump supplier.

Source: <http://www.detroitnews.com/story/business/autos/foreign/2015/04/10/nissan-bmw-recall-vehicles-fuel-pump/25566297/>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

5. *April 9, U.S. Securities and Exchange Commission* – (International) **SEC announces fraud charges against former accounting executive at Japanese subsidiary.** The U.S. Securities and Exchange Commission charged the former controller of Lisle-based Molex Japan Co. Ltd., a Japanese subsidiary of Molex Incorporated, with fraud April 9 after he allegedly caused the company \$201.9 million in net losses through unauthorized equity trading in the company's brokerage accounts, which he tried to conceal by falsifying records and taking out unauthorized loans with Japanese banks and brokerage firms to replenish the funds and engage in further trading.
Source: <http://www.sec.gov/news/pressrelease/2015-65.html>
6. *April 9, U.S. Securities and Exchange Commission* – (Florida; New York) **SEC halts microcap scheme in South Florida.** The U.S. Securities and Exchange Commission announced fraud charges and an asset freeze April 9 against the CEO and 3 sales agents of Boca Raton-based eCareer Holdings, Inc., in a microcap scheme in which they allegedly defrauded over 400 investors out of more than \$11 million since 2010 by selling unregistered stock shares in the company, falsely advertising the shares as a profitable investment, and concealing the exorbitant fees being paid to the sales agents.
Source: <http://www.sec.gov/news/pressrelease/2015-63.html>
7. *April 8, CBS News* – (National) **Federal agency sues collectors of “phantom debt”.** The Consumer Financial Protection Bureau unsealed a March 26 lawsuit April 9 against two Georgia men, co-conspirators, and 7 debt collection companies following allegations that the firms used cold calls to convince millions of consumers to pay debts they did not owe through tactics that involved purchasing personal information such as bank account numbers from data brokers. A telemarketing company and several payment processing companies were also charged in the scheme.
Source: <http://www.cbsnews.com/news/federal-agency-sues-collectors-of-phantom-debt/>

[\[Return to top\]](#)

Transportation Systems Sector

8. *April 10, WCHS 8 Charleston* – (Ohio) **One eastbound lane open on U.S. 52 near boulder collapse.** Ohio Department of Transportation officials reported April 10 that both westbound lanes of U.S. 52 near Coal Grove could remain closed for several days after a 20-foot-tall boulder fell and blocked the roadway. One lane of eastbound traffic reopened after crews cleared debris from the roadway several hours after the boulder collapse.
Source: <http://www.wchstv.com/news/features/eyewitness-news/stories/Boulder-closes-U-S-Route-52-near-Ashland-Bridges-113444.shtml>
9. *April 10, San Francisco Chronicle* – (California) **Crash closes I-580 lanes west of Richmond-San Rafael Bridge.** One eastbound lane of Interstate 580 near the Richmond-San Rafael Bridge reopened after closing for nearly 5 hours April 10 after a United Parcel Service semi-truck crashed into a median and caught fire. Westbound lanes were expected to remain closed for at least 8 hours.
Source: <http://www.sfgate.com/news/article/Crash-closes-I-50-west-of-Richmond-San-Rafael-6191447.php>
10. *April 10, KCRA 3 Sacramento* – (California) **All lanes open on Hwy. 12 after deadly crash in San Joaquin County.** Highway 12 in San Joaquin County was closed in both directions for approximately 4 hours April 10 while crews cleared the scene of a fatal accident.
Source: <http://www.kcra.com/news/local-news/news-sacramento/deadly-crash-closes-section-of-hwy-12-in-san-joaquin-county/32298174>
11. *April 10, Philly.com* – (Pennsylvania) **All lanes reopen on Ben Franklin Bridge after tractor-trailer crash.** All lanes of the Benjamin Franklin Bridge reopened after 2 westbound lanes heading into Philadelphia were closed for more than 3 hours April 10 while crews cleared the scene after a semi-truck overturned.
Source: http://www.philly.com/philly/news/Overtuned_tractor-trailer_causing_delays_on_Ben_Franklin_Bridge.html
12. *April 8, U.S. Environmental Protection Agency* – (Missouri) **Missouri Department of Transportation to implement statewide compliance program to settle construction stormwater violations.** The U.S. Environmental Protection Agency (EPA) reported April 8 that the Missouri Department of Transportation agreed to pay \$750,000 in fines and implement a Statewide compliance program to settle alleged Clean Water Act violations at the site of 2 road building projects in 2010 and 2011. The alleged violations took place at construction sites along Highway 54 in Osage Beach and Highway 67 between Coldwater and Silva, where EPA inspectors found unsatisfactory stormwater control measures and negligence in repairing those that were installed, among other findings.
Source: <http://yosemite.epa.gov/opa/admpress.nsf/0/1E4958DFFD55324185257E21006C0501>

For another story, see item [30](#)

Food and Agriculture Sector

13. *April 9, U.S. Food and Drug Administration* – (National) **Texas Pecan Company voluntarily recalls macadamia nuts and products containing macadamia nuts because of possible Salmonella contamination.** The U.S. Food and Drug Administration reported April 9 that Texas Pecan Company Inc., voluntarily recalled certain packaged macadamia nuts and gift tins containing macadamia nuts due to possible Salmonella contamination. The recalled products were distributed through the company's Dallas-based retail store and via mail orders nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm442042.htm>
14. *April 9, KTVB 7 Boise* – (Idaho) **Boise restaurant shut down by health department.** Pho Tam, a Boise restaurant, was ordered closed April 9 by Idaho's Central District Health Department after an investigation revealed four critical health code violations, including two repeat violations. The investigation was initiated following a suspected Salmonella outbreak that sickened five guests between February and March.
Source: <http://www.ktvb.com/story/news/health/2015/04/09/pho-tam-health-code-violations/25544545/>
15. *April 9, Forum of Fargo-Moorhead* – (Minnesota) **Bull semen worth \$70,000 stolen from Minnesota farm.** The Mower County Sheriff's Office is searching for \$70,000 worth of cryogenically frozen bull semen and about \$30,000 worth of frozen embryos that were stolen from an unlocked barn at a farm in Minnesota the week of April 6.
Source: <http://www.duluthnewstribune.com/news/3718828-bull-semen-worth-70000-stolen-minnesota-farm>
16. *April 9, Joplin Globe* – (Missouri; Arkansas; Kansas) **Missouri lifts avian flu quarantines.** The Missouri Department of Agriculture announced April 9 that a poultry quarantine in connection with the H5N2 avian influenza was lifted in Moniteau and Jasper counties after surveillance and testing yielded results that show no further spread of the virus. Quarantines in Boone County, Arkansas, and Leavenworth and Wyandotte counties in Kansas were also lifted within the past week.
Source: http://www.joplinglobe.com/news/local_news/missouri-lifts-avian-flu-quarantines/article_dc10d4cd-2e0f-5138-8a1f-b8a135289d7b.html
17. *April 9, Associated Press* – (South Dakota) **Second commercial turkey flock in SD found with avian influenza.** The U.S. Department of Agriculture confirmed April 9 the presence of the H5N2 strain of avian influenza in a commercial flock of 34,000 turkeys in Kingsburg County. The farm was quarantined by State officials, and birds on the property will be culled to prevent the spread of the disease.
Source: <http://www.ksfy.com/home/headlines/Second-commercial-turkey-in-SD-found-with-avian-influenza-299228971.html>

Water and Wastewater Systems Sector

18. *April 9, San Francisco Bay Area News* – (California) **Cleanup underway after huge cement spill into Oakland hills creek.** The East Bay Municipal Utility District (EBMUD) reported that about 12 truckloads of cement accidentally spilled into the Rockridge Branch of the Glen Echo Creek watershed April 8 when EBMUD crews that were repairing pipes in Oakland left a valve on a truck partially open. A contractor was hired to pump cement out of a 1,000-foot stretch of the creek that was clogged by the spill, while authorities continue to search the waterway for injured wildlife and possible environmental impacts.

Source: http://www.contracostatimes.com/breaking-news/ci_27879317/oakland-cement-spill-clogs-creek-hills

[\[Return to top\]](#)

Healthcare and Public Health Sector

19. *April 10, KYTX 19 Nacogdoches* – (Texas) **Eden Select Specialty Care in Longview evacuate after storm.** All 75 patients of Eden Select Specialty Care in Longview were evacuated and transported to other facilities in the area after a severe storm April 9 damaged the roof of the facility.

Source: <http://www.cbs19.tv/story/28767542/longview-pd-evacuating-eden-select-specialty-care>

[\[Return to top\]](#)

Government Facilities Sector

20. *April 10, WRC 4 Washington, D.C.* – (Washington, D.C.; Maryland) **Guard dead after shooting at U.S. Census Bureau headquarters.** A gunman was wounded April 9 following an exchange of gunfire between the suspect and police after the man kidnapped his wife in Washington, D.C., drove to the U.S. Census Bureau headquarters in Suitland, Maryland, and fatally shot a security guard that approached his vehicle. Authorities spotted and pursued the suspect's car before exchanging gunfire that also left a Washington, D.C. police officer injured.

Source: <http://www.nbcwashington.com/news/local/Report-Shooting-Census-Bureau-Headquarters-in-Md-299259981.html>

21. *April 10, Pasco Tribune; Tampa Tribune* – (Florida) **Pasco student accused of unauthorized access to school computers.** Officials announced that a student from Paul R. Smith Middle School in Pasco County was charged after allegedly gaining access to a school computer containing Florida Comprehensive Assessment Test data, and gaining access to a substitute teacher's computer. The school district is investigating how the student was able to obtain the password and remotely log in to the system.

Source: <http://tbo.com/pasco-county/pasco-student-accused-of-unauthorized-access-to-school-computers-20150409/>

22. *April 9, Milpitas Post* – (California) **All clear given after bomb threat forces evacuation of Milpitas High School.** Students were evacuated and classes were dismissed at Milpitas High School in California April 9 due to a bomb threat left on the school's voice mail. Police cleared the scene after nearly 4 hours once nothing suspicious was found.

Source: http://www.mercurynews.com/milpitas/ci_27879862/breaking-news-bomb-threat-forces-evacuation-milpitas-high

[\[Return to top\]](#)

Emergency Services Sector

23. *April 9, WDIV 4 Detroit* – (Michigan) **Detroit police officers accused of stealing, selling drugs.** Two Detroit police officers were charged with allegedly setting up drug transactions with civilians in order to rob and extort them, in addition to carrying out traffic stops and fake arrests set up to rob people of drugs, money, and personal property. The pair have been suspended from duty since October 2014 after an investigation determined they would carry out the crimes dressed as law enforcement officers.

Source: <http://www.clickondetroit.com/news/detroit-police-officers-accused-of-stealing-selling-drugs/32276694>

[\[Return to top\]](#)

Information Technology Sector

24. *April 10, Softpedia* – (International) **OS X 10.9.x and older vulnerable to hidden backdoor API.** A Swedish security researcher discovered a hidden backdoor application programming interface (API) present in the Admin framework of Apple OS X versions prior to 10.10.2 that could grant attackers root access to users with both admin and regular user accounts. Apple patched the issue in its release of OS X 10.10.3

Source: <http://news.softpedia.com/news/OS-X-10-9-x-and-Older-Vulnerable-to-Hidden-Backdoor-API-478136.shtml>

25. *April 10, Softpedia* – (International) **United States, South Africa most affected by Changeup worm.** A task force of European and American law enforcement organizations and private security companies including Intel, Kaspersky, and Shadowserver took action to disrupt the Changeup worm botnet and sinkhole its command-and-control (C&C) servers. The worm morphed every few hours and leveraged a LNK vulnerability in Windows to infect approximately 30,000 systems in early 2015, and downloaded other pieces of malware including banking trojans, click-fraud programs, crypto-malware and other botnet threats.

Source: <http://news.softpedia.com/news/United-States-South-Africa-Most-Affected-By-Changeup-Worm-478175.shtml>

26. *April 9, Softpedia* – (International) **Multiple flaws found in Motorola's Surfboard SBG6580 cable modem.** Security researchers at Rapid7 discovered vulnerabilities in

Motorola Home/ARRIS Surfboard SBG6580 series cable modems including a backdoor account with hardcoded credentials and persistent cross-site scripting (XSS) and cross-site request forgery (CSRF) flaws that could allow attackers that know the internal gateway internet protocol (IP) address to access the device remotely, change network settings, and inject malicious JavaScript (JS) code.

Source: <http://news.softpedia.com/news/Multiple-Flaws-Found-in-Motorola-s-Surfboard-SBG6580-Cable-Modem-478071.shtml>

27. *April 9, Softpedia* – (International) **Cisco threat defense tool vulnerable to DoS attack.** Cisco released a security advisory that a flaw in the company's ASA FirePOWER and Context Aware (CX) Services can be exploited to allow attackers to cause denial-of-service (DoS) conditions by sending a high rate of crafted packets to the services' management interface. Cisco released updates for the products addressing the issues as well as three additional related glitches.

Source: <http://news.softpedia.com/news/Cisco-Threat-Defense-Tool-Vulnerable-to-DoS-Attack-478082.shtml>

28. *April 9, Softpedia* – (International) **Group uses over 300,000 unique passwords in SSH log-in brute-force attacks.** Security researchers from Cisco Talos Group and Level 3 Communications collaborated to monitor and take down netblocks being used by a group of cybercriminals dubbed SSHPsychos to run large amounts of scamming traffic, utilizing a dictionary to find root user log-in credentials and install distributed denial-of-service (DDoS) rootkits that add compromised systems to a persistent DDoS botnet.

Source: <http://news.softpedia.com/news/Group-Uses-Over-300-000-Unique-Passwords-in-SSH-Log-In-Brute-Force-Attacks-478094.shtml>

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

29. *April 9, KIRO 7 Seattle* – (Washington) **Comcast service restored to 33,000 customers.** Internet, phone, and cable service was restored to about 33,000 Comcast customers in the Seattle area after a damaged fiber optic line knocked out service for several hours April 9. Customers who could not access 9-1-1 emergency services from a landline were advised to call from a mobile phone in case of an emergency.

Source: <http://www.kirotv.com/news/news/comcast-customers-report-outages-seattle/nkqfx/>

[\[Return to top\]](#)

Commercial Facilities Sector

30. *April 10, St. Louis Post-Dispatch* – (Missouri; Illinois) **Storms damage about 15 buildings in Chesterfield near airport, flood Madison County roads.** Severe storms passing through the St. Louis area April 8-9 damaged about 15 buildings in a light industrial business area in Chesterfield, and knocked out power to about 26,000 customers. The storm also killed 1 person and injured 7 others while causing damage to approximately 50 structures in Fairdale, Illinois.
Source: http://www.stltoday.com/news/local/crime-and-courts/storms-damage-buildings-in-chesterfield-near-airport-flood-madison-county/article_6de323a5-face-551a-a1f7-d044e185e6bd.html
31. *April 9, Associated Press* – (New York) **Police: Man stole \$1M-plus from Tioga County employer.** A Waverly, New York man was arrested April 2 and charged with stealing more than \$1 million from his former employer, Straight Line LLC, after a year-long investigation revealed the falsification of business records and misappropriation of vehicle ownership documents.
Source: <http://www.oneidadispatch.com/general-news/20150409/police-man-stole-1m-plus-from-tioga-county-employer>
32. *April 9, WJAR 10 Providence* – (Rhode Island) **50 people driven out by fire in Woonsocket complex.** Authorities are investigating a 3-alarm fire that severely damaged an apartment complex in Woonsocket April 8 and displaced about 50 residents. No injuries were reported.
Source: <http://www.turnto10.com/story/28758308/35-people-driven-out-by-fire-in-woonsocket-complex>

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.